DEPARTMENT OF NATIONAL DEFENCE

CANADA

DIRECTORATE OF STRATEGIC ANALYSIS

POLICY GROUP

RESEARCH NOTE NO. 98/09

# INFORMATION WARFARE

# AND

# INFORMATION OPERATIONS

by

Dr. Elinor C. Sloan

October 1998

OTTAWA, CANADA

National Defence | Défense nationale

## OPERATIONAL RESEARCH DIVISION

## CATEGORIES OF PUBLICATION

**ORD Reports** are the most authoritative and most carefully considered publications of the DGOR scientific community. They normally embody the results of major research activities or are significant works of lasting value or provide a comprehensive view on major defence research initiatives. ORD Reports are approved personally by DGOR, and are subject to peer review.

**ORD Project Reports** record the analysis and results of studies conducted for specific sponsors. This Category is the main vehicle to report completed research to the sponsors and may also describe a significant milestone in ongoing work. They are approved by DGOR and are subject to peer review. They are released initially to sponsors and may, with sponsor approval, be released to other agencies having an interest in the material.

**Directorate Research Notes** are issued by directorates. They are intended to outline, develop or document proposals, ideas, analysis or models which do not warrant more formal publication. They may record development work done in support of sponsored projects which could be applied elsewhere in the future. As such they help serve as the corporate scientific memory of the directorates.

**ORD Journal Reprints** provide readily available copies of articles published with DGOR approval, by OR researchers in learned journals, open technical publications, proceedings, etc.

**ORD Contractor Reports** document research done under contract of DGOR agencies by industrial concerns, universities, consultants, other government departments or agencies, etc. The scientific content is the responsibility of the originator but has been reviewed by the scientific authority for the contract and approved for release by DGOR.

106-03407/

**DIRECTORATE OF STRATEGIC ANALYSIS**

RESEARCH NOTE NO. 98/09

# INFORMATION WARFARE

# AND

# INFORMATION OPERATIONS

by

Dr. Elinor C. Sloan

Directorate Project Reports present the considered results of analysis to interested agencies. They do not necessarily represent the official views of the Department of National Defence.

OTTAWA, CANADA October 1998

## TABLE OF CONTENTS


ABSTRACT/RÉSUMÉ ..... ii
EXECUTIVE SUMMARY ..... iii
SOMMAIRE ..... v

**Introduction** ..... 1

**What is information warfare?** ..... 1
Intelligence-based warfare ..... 2
Command and control warfare ..... 3
Electronic warfare ..... 5
Computer network attack or hacker warfare ..... 5
Psychological warfare ..... 6
Offensive and defensive information warfare ..... 7

**US service visions and information warfare** ..... 8

**Is information warfare new?** ..... 9

**Information operations** ..... 10
Computer network attack on civilian systems ..... 11
Threats and vulnerabilities ..... 13
Threats to military information systems ..... 13
Threats to civilian information systems ..... 14
Private sector perspective ..... 15
Military and intelligence perspective ..... 16
Deterring computer network attack ..... 17
Defending against computer network attack ..... 18

**Conclusion** ..... 19

## ABSTRACT/SOMMAIRE

This report begins by looking at the definition, objective and forms of information warfare. It then discusses the role of information warfare in military operations before turning to the broader concept of information operations. Here the paper focuses on the prospect of a computer network attack on civilian infrastructures and how governments are responding. The report concludes that the challenge of the future is not only to find effective responses to, and ways of conducting, information operations, but also to define the responsibilities and identify the appropriate agencies for carrying out these tasks.

En premier lieu, ce rapport présente la définition, l'objectif et les diverses formes de la guerre de l'information. Il explique ensuite le rôle que joue la guerre de l'information dans les opérations militaires, puis décrit le concept plus large des opérations d'information. Il se poursuit en abordant l'éventualité d'une attaque des réseaux informatiques appartenant aux infrastructures civiles et la façon dont les gouvernements s'y préparent. Le rapport conclut que la lourde tâche qu'il faudra accomplir au cours des prochaines années consistera non seulement à trouver des moyens d'agir efficacement face aux opérations d'information et de mener ce genre d'opérations, mais aussi à définir les responsabilités en la matière et à déterminer les organismes qui pourront relever ce défi.

## EXECUTIVE SUMMARY

1. Today information technology is just as crucial for the efficient prosecution of a war effort as it is for the smooth functioning of stock markets and air traffic control towers. As advanced military forces and societies become ever more dependent on information technology, vulnerabilities inevitably arise which an opponent could exploit. This prospect raises the spectre of information warfare during actual conflict and information operations spanning the entire period of confrontation.

2. Information warfare is actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems and computer-based networks. Its objective is to attain a significant information advantage that enables a military force to quickly dominate and control the adversary. Forms of information warfare include intelligence-based warfare, command and control warfare, computer network attack, electronic warfare and psychological operations.

3. Intelligence-based warfare refers to those activities that produce battlespace awareness—the ability to collect and transmit data, integrate and assess the data, and plan actions based on that understanding. Battlespace awareness rests on advanced sensing and reporting technologies. Command and control warfare is attacks against the "head and neck" of an adversary in order to sever the enemy's command structure from its body of command forces. It is traditionally waged by inflicting physical destruction, but in the future may also be carried out through computer network attack. This form of warfare, also known as "hacker warfare", refers to software-based attacks on information systems. It corrupts information without visibly changing the physical entity within which it resides. Electronic warfare is attacks within the electromagnetic spectrum on the enemy's sensor and communications systems. It can be used both to blind the opponent and cut off commanders from their troops. Finally, psychological operations are operations designed to influence the behaviour, attitudes and emotions of a target foreign audience.

4. Offensive information warfare is measures designed to exploit or degrade an adversary's ability to collect or use information. It includes traditional methods such as precision attacks to destroy an adversary's command and control capability, and nontraditional methods like attacking with computer viruses and managing information through media deception. Defensive information warfare, by contrast, protects one's own ability to carry out information-based operations. Traditional defensive information warfare activities include physical security measures and encryption; nontraditional actions will range from antivirus protection to innovative methods of secure data transmission.

5. The pervasiveness of information technology is such that its role needs to be understood not just in terms of actual warfighting but also in the context of the broader information environment. The Canadian Forces Information Operations doctrine document

defines information operations as actions taken in support of political and military objectives which influence decision makers by affecting others' information while exploiting and protecting one's own information. Such actions might include a computer network attack on civilian systems, a public affairs campaign or, if the confrontation has escalated to a conflict, the information warfare techniques discussed above. Information operations can be viewed as an overarching concept which subsumes information warfare as one of its components.

6. One much-discussed aspect of information operations is the notion of a computer network attack on civilian computer-based systems. Many military and intelligence officials in the United States and Canada believe that such an attack is a distinct possibility. Potential targets include electrical power grids, telephone systems, stock markets, financial centres and the air traffic control system. Possible attackers range from hostile national intelligence and military organizations to terrorists, criminals, industrial competitors and disgruntled or disloyal insiders. Because they are designed for public access, civilian systems are comparatively easier to penetrate than military ones. A computer network attack on civilian systems could have direct military implications since many of the things the military does depends on civilian information networks. In the United States, 95 per cent of military communications are done over civilian phone lines.

7. Both the United States and Canada have undertaken initiatives to increase the security of civilian infrastructures. The US President created a Commission on Critical Infrastructure Protection in 1996 and two years later issued a directive implementing the Commission's key recommendations, including the creation of an Office of National Infrastructure Assurance within the National Security Council. Meanwhile, the Pentagon has established an Information Operations Working Group to address defence-related issues of infrastructure protection. As for Canada, DND has approved a doctrine document on Canadian Forces Information Operations providing guidance on all aspects of information operations. In addition, a CF Information Operations Group has been created and both a Network Vulnerability Assessment Team and a Computer Instant Response Team have been established. Finally, Canada is participating in the Pentagon's working group on information operations.

8. The prospect of a computer network attack on civilian infrastructure serves to blur the traditional distinction between domestic law enforcement and national security. In Canada, this could lead to confusion over the division of responsibilities between the Solicitor General and the Department of National Defence. For its part, DND has underlined that when it comes to infrastructure protection, departmental responsibilities are limited to defence works, establishments, facilities, assets, resources and operations, in Canada and abroad. The Department has consistently advocated a strong centrally based leadership role for the Privy Council Office in the area of infrastructure protection. The challenge of the future will not only be to find effective responses to, and ways of conducting, information operations, but also to define the responsibilities and identify the appropriate agencies for carrying out these tasks.

## RÉSUMÉ ANALYTIQUE

1. Aujourd'hui, la technologie de l'information est aussi vitale pour soutenir un effort de guerre que pour assurer le bon fonctionnement des marchés boursiers et des tours de contrôle de la circulation aérienne. Plus les forces militaires et les sociétés modernes deviennent dépendantes de la technologie de l'information, plus elles présentent des failles dont leurs adversaires pourraient tirer parti. Il se peut donc qu'une guerre de l'information éclate lors d'un conflit et qu'il soit nécessaire de mener des opérations d'information durant toute la période de confrontation.

2. La guerre de l'information représente les mesures que prend un pays pour établir sa supériorité dans le domaine de l'information en portant atteinte à l'information, aux processus informationnels, aux systèmes d'information et aux réseaux informatiques de l'adversaire, tout en protégeant ses propres sources d'information et ses processus informationnels, ses systèmes d'information et ses réseaux informatiques. La guerre de l'information a pour objectif d'obtenir un avantage suffisant dans le domaine de l'information pour permettre aux forces militaires de dominer et de contrôler rapidement l'adversaire. Elle peut prendre diverses formes : guerre du renseignement, guerre de commandement et de contrôle, attaque de réseaux informatiques, guerre électronique et opérations psychologiques.

3. La guerre du renseignement regroupe les activités qui favorisent la sensibilisation à l'espace de bataille—la capacité de recueillir et de transmettre des données, d'intégrer et d'évaluer ces données et de planifier des mesures en conséquence. La sensibilisation à l'espace de bataille repose sur les hautes technologies de détection et de transmission de données. La guerre de commandement et de contrôle consiste à attaquer «le cerveau» de l'adversaire afin que ses forces de commandement n'aient plus de structure de commandement. Ce type de guerre est menée en général au moyen de mesures de destruction matérielle, mais, dans l'avenir, elle se fera peut-être aussi par l'intermédiaire des réseaux informatiques. Cette forme de guerre, qu'on appelle également «sabotage informatique», consiste à attaquer des systèmes d'information à partir de logiciels, l'information étant altérée sans que les installations physiques dans lesquelles elle est stockée ne soient endommagées. La guerre électronique consiste à attaquer les systèmes de détection et de communication de l'ennemi à l'intérieur du spectre électromagnétique. Elle peut servir à aveugler l'adversaire et à couper les commandants de leurs troupes. Enfin, les opérations psychologiques visent à influencer le comportement, les attitudes et les émotions de groupes cibles étrangers.

4. La guerre de l'information offensive consiste à exploiter ou à diminuer la capacité de l'adversaire de recueillir ou d'utiliser de l'information. Elle fait appel entre autres à des méthodes traditionnelles, comme les attaques de précision visant à détruire la capacité de commandement et de contrôle de l'adversaire, et à des méthodes peu traditionnelles, comme les attaques à l'aide de virus informatiques et la gestion de l'information visant à tromper les

médias. La guerre de l'information défensive vise plutôt à protéger sa propre capacité de réaliser des opérations d'information. Les mesures de sécurité physique et le cryptage sont quelques moyens défensifs traditionnels. Les mesures non traditionnelles varient de la protection antivirus aux méthodes novatrices de transmission protégée de données.

5. Parce que la technologie de l'information est omniprésente, il est crucial de comprendre le rôle qu'elle joue non seulement dans le cadre des combats proprement dits, mais aussi dans le contexte global de l'information. Le document de doctrine sur les opérations d'information des Forces canadiennes définit les opérations d'information comme étant les mesures prises en vue d'appuyer les objectifs politiques et militaires qui influencent ceux qui prennent les décisions en altérant l'information dont dispose l'adversaire tout en exploitant et en protégeant ses propres sources d'information. Ces opérations peuvent prendre la forme d'une attaque contre des systèmes informatiques civils ou d'une campagne d'affaires publiques. Si la confrontation dégénère en conflit, on peut avoir recours aux techniques de guerre de l'information énumérées ci-dessus. En gros, on peut dire que les opérations d'information représentent le concept général qui englobe la guerre de l'information.

6. Un des aspects des opérations d'information dont on parle beaucoup est l'éventualité d'une attaque des réseaux informatiques civils. De nombreux militaires et responsables du renseignement aux États-Unis et au Canada pensent qu'une attaque de ce genre est très possible. Parmi les cibles éventuelles se trouvent les réseaux électriques, les systèmes téléphoniques, les marchés boursiers, les centres financiers et les systèmes de contrôle de la circulation aérienne. Ce genre d'attaque pourrait être lancée par des organismes du renseignement et des organisations militaires de pays hostiles aussi bien que par des terroristes, des criminels, des compétiteurs industriels ou des personnes de l'intérieur mécontentes ou déloyales. Étant donné que les systèmes civils sont accessibles au public, il sont plus faciles à infiltrer que les systèmes militaires. Une attaque dirigée contre des systèmes civils risque de toucher directement les forces militaires, car ces dernières dépendent des réseaux informatiques civils sur de nombreux plans. Aux États-Unis par exemple, 95 p. 100 des communications militaires se font par les lignes téléphoniques civiles.

7. Les États-Unis et le Canada ont pris des mesures afin d'améliorer la sécurité de leurs infrastructures civiles. En 1996, le président des É.-U. a créé la Commission on Critical Infrastructure Protection. Deux ans plus tard, il a émis une directive afin de mettre en oeuvre les recommandations clés de la commission, ce qui a donné lieu entre autres à la création d'un Office of National Infrastructure Assurance au sein du National Security Council. Entre-temps, le Pentagone a formé un groupe de travail sur les opérations d'information en vue de traiter les questions de protection de l'infrastructure qui touchent la défense. Au Canada, le MDN a approuvé le document de doctrine sur les opérations d'information des Forces canadiennes, qui énonce des directives sur tous les aspects des opérations d'information. Également, on a mis sur pied le Groupe des opérations d'information des FC

ainsi que l'Équipe d'évaluation de la vulnérabilité des réseaux et l'Équipe d'intervention en cas d'incident informatique. Enfin, le Canada fait partie du groupe de travail du Pentagone sur les opérations d'information.

8. L'éventualité d'une attaque des réseaux informatiques de l'infrastructure civile vient brouiller la distinction traditionnelle entre l'application de la loi au niveau national et la sécurité nationale. Au Canada, cela risque de créer de la confusion au sujet de la répartition des responsabilités entre le Solliciteur général et le ministère de la Défense nationale. Pour sa part, le MDN a précisé que, au chapitre de la protection de l'infrastructure, ses responsabilités sont limitées aux ouvrages, aux établissements, aux installations, aux biens, aux ressources et aux opérations relevant de la défense, au Canada et à l'étranger. Le Ministère s'est toujours montré favorable à ce que le Bureau du Conseil privé joue un rôle central dominant à l'égard de la protection de l'infrastructure. La tâche qu'il faudra accomplir au cours des prochaines années consistera non seulement à trouver des moyens d'agir efficacement face aux opérations d'information et de mener ce genre d'opérations, mais aussi à définir les responsabilités en la matière et à déterminer les organismes qui pourront relever ce défi.

# INFORMATION WARFARE AND INFORMATION OPERATIONS

## INTRODUCTION

1. Information technology is increasingly central to military and civilian life. Today information technology is just as crucial for the efficient prosecution of a war effort as it is for the smooth functioning of stock markets and air traffic control towers. As advanced military forces and societies become ever more dependent on information technology, vulnerabilities inevitably arise which an opponent could exploit. This prospect raises the spectre of information warfare during actual conflict and information operations spanning the entire period of confrontation.

2. This paper outlines the various forms of information warfare. It then looks briefly at the role of information warfare in military operations before turning to the broader concept of information operations. Here the paper focuses on a specific aspect of information operations—vulnerabilities and threats of computer network attack on civilian infrastructures and how governments are responding.

## WHAT IS INFORMATION WARFARE?

3. Information warfare is defined by the Office of the Chairman of the US Joint Chiefs of Staff as "actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems and computer-based networks."[1] Information warfare has been similarly defined in a Canadian context as "actions taken to achieve a goal by influencing and controlling adversary information, computer processes and information systems, while protecting one's own information, computer

[1] United States Army Field Manual 100-6, *Information Operations*, August 1996, p. 2-2.

and information systems."[2]

4. The overall objective of information warfare is "to attain a significant information advantage that enables the total force to quickly dominate and control the adversary."[3] The goal, in short, is to achieve information superiority, and through that to secure a situation of information dominance. Information dominance is defined by the US Army as "the degree of information superiority that allows the possessor to use information systems and capabilities to achieve an operational advantage in a conflict, while denying those capabilities to the adversary."[4] More simply, information dominance consists of "knowing everything about the adversary while keeping the adversary from knowing much about oneself."[5] Actions taken to achieve information superiority and dominance may encompass a number of different forms of warfare, each of which is often referred to synonymously as "information warfare," but is better understood as a specific type, or sub-category, of information warfare.

**Intelligence-based warfare**

5. Key to achieving information superiority is intelligence-based warfare. This type of warfare refers to those activities that produce battlespace awareness—the ability to "see" (collect and transmit data), "understand" (be able to integrate and assess data) and "know" (plan actions based on that understanding) the battlespace.[6] Battlespace awareness rests on sensing and reporting technologies and includes both the platforms and sensors that are associated with intelligence gathering, surveillance and reconnaissance, and the reporting systems that provide better awareness of, and communications with, one's own forces.[7]

---

[2] Annex B to *Information Warfare and the Canadian Forces*, 9 May 1996, http://www.dnd.ca/diso/library/lib_e.htm.

[3] *Information Operations*, p. 2-2.

[4] Ibid., p. 1-9.

[5] John Arquilla and David Ronfeldt, "Cyberwar is Coming!" *Comparative Strategy*, Vol. 12, 1993, p. 146.

[6] Patricia M. Barwinczak, "The Information Revolution and Warfare 2020," *Strategic Review*, Spring 1997, p. 77.

[7] William A. Owens, "The Emerging System of Systems," *Military Review*, May-June 1995, p. 17.

6. Sensing technologies are found on satellites, manned aircraft and, increasingly, unmanned aircraft. The manned Joint Surveillance Target Attack Radar System and Airborne Warning and Control Systems provide surveillance of the ground and airspace respectively. In the future, unmanned aerial vehicles, such as America's medium-altitude *Predator* and high-altitude *Global Hawk*, are also expected to be used to achieve battlespace awareness. An example of an advanced reporting system is the US Air Force's Joint Situational Awareness System which, unlike previous command and control systems, merges battlefield intelligence gathered by spy satellites, commercial satellites, U-2 reconnaissance aircraft, AWACS, JSTARS and *Predator* unmanned surveillance aircraft.[8]

7. During the Gulf War, the US-led coalition enjoyed an information advantage as a result of a communications network that linked satellites, observation aircraft and commanders. Nonetheless, the numerous sophisticated reconnaissance, communications and targeting systems still had difficulty communicating with one another.[9] To address this problem, US Admiral William Owens has outlined a vision of a "system of systems" in which systems that provide for battlespace awareness, the use of precision force, and advanced command, control and communications, use more compatible software and hardware, thereby dramatically boosting their synergism and effectiveness.[10] This vision is slowly being implemented in the United States.

**Command and control warfare**

8. Intelligence-based warfare is an important precursor to command and control warfare. This term refers to attacks against the "head and neck"[11] of an adversary in order to "decapitate

---

[8] Steven Watkins, "USAF System Links Battlefield Intelligence Data," *Defense News*, 12–18 August 1997, p. 12.

[9] *Economist* Survey on Defence Technology, 10 June 1995, p. 8.

[10] Owens, p. 17.

[11] Martin Libicki, *What is Information Warfare?* (Washington, D.C.: National Defense University Institute for National Strategic Studies), August 1995, http://198.80.36.91/ndu/inss/actpubs/act003/a003cont.html.

the enemy's command structure from its body of command forces."[12] Intelligence-based warfare prepares the battlefield for command and control warfare, providing commanders with the essential targeting information and battle damage assessment without which command and control warfare could not be waged effectively.

9. One way in which command and control warfare can be waged is by inflicting physical destruction. In the initial stages of the Gulf War, for example, air strikes were conducted against Iraqi command, control, communications and intelligence targets. Coalition navies and air forces used precision-guided munitions to bomb Iraqi telephone exchanges, command and control nodes, radar sites and other vital information and communications links. The theory behind this action was that "if we could sever leaders from their troops [by using air power], we wouldn't have to fight them in the field."[13] In the future, better intelligence could enable forces to conduct precision strikes against key computer systems and leave other systems untouched.[14]

10. The future may also see weapons of pure information—such as computer viruses—used for command and control warfare.[15] An all-out on-line attack from a network penetration designed to collapse a military information structure could cut off troops from their commanders, and commanders from their national authorities.[16] Such a scenario would see a computer terminal replacing the airplane, "logic bombs" replacing the ordnance and the "enter" key replacing the trigger.[17]

---

[12] US Department of Defense Directive TS-3600.1, 21 December 1992, *Information Warfare*, as quoted in Libicki.

[13] Pat Cooper, "C3I, Data Become Battlefield Targets," *Defense News*, 4-10 December 1995, p. 8.

[14] Pat Cooper, "Information Warfare Operations Require Intelligence Boost," *Defense News*, 9-15 September 1996, p. 16.

[15] *Economist* Survey on Defence Technology, p. 19.

[16] Pat Cooper, "Pentagon Debates Potential of Information Warfare," *Defense News*, 13-19 May 1996, p. 3.

[17] John A. Tirpak, "The New World of Information Warfare," *Air Force Magazine*, June 1996, p. 32.

**Electronic warfare**

11. A third form of information warfare is electronic warfare. This term refers to attacks within the electromagnetic spectrum on the enemy's sensor and communications systems. "Control the electromagnetic dimension of the battlefield, goes today's wisdom, and you are most of the way to controlling it all."[18] Electronic warfare complements both intelligence-based warfare and command and control warfare in that it can be used both to blind the opponent and to cut off commanders from their troops.

12. Any channel of communication found in the electromagnetic spectrum can be disrupted by jamming.[19] Jammers can clog military radio links and electromagnetic pulse weapons can burn out enemy electronics. During the Gulf War, the US Army's Sandcrab jammer disrupted long-range radio links throughout Iraq.[20] In the future, an aircraft's communications system might be crippled by electromagnetic pulses or high-power microwaves.[21]

**Computer network attack or hacker warfare**

13. Computer network attack, also known as "hacker warfare" refers to software-based attacks on information systems.[22] These attacks directly corrupt information without visibly changing the physical entity within which it resides.[23] As a result, a computer network attack can take place without the enemy's realizing it.

14. Computer network attack has a number of potential military applications. By inserting

---

[18] *Economist* Survey on Defence Technology, p. 8.

[19] *Economist* Survey on Defence Technology, p. 11.

[20] Neil Munro, "The Pentagon's New Nightmare: An Electronic Pearl Harbour," *Defense News*, 16 July 1995, p. C3.

[21] Tirpak, p. 34.

[22] Gregory J. Walters, "A New Way of War in the Information Age," *Ottawa Citizen*, 14 March 1998, p. B7.

[23] US Air Force, *Cornerstones of Information Warfare*, Fall 1995, http://www.af.mil/lib/corner.html.

codes that cause software to function improperly the information warrior could change targeting information on military systems, causing missiles to miss their targets or to rain back on the belligerent nation—without ever alerting the target nation that their computers had been breached.[24] Similarly, if military hackers were able to get into the database of a ground or airborne system and change it, the result could a plane's sensors "recognizing " friendly aircraft as enemy or switching the target coordinates for a standoff missile.[25] Other scenarios see enemy ships sent to the wrong area, troops lulled into vulnerability with false threat assessments and military planners sent to the wrong places for fabricated reasons.[26] Information warriors may even be able to deny the enemy the true picture offered by sensors and radar systems, causing him to fight blindly, all the while thinking that he has an accurate picture of the battlefield.[27]

**Psychological warfare**

15. A final form of information warfare is *psychological operations*—or psyops—which refer to operations designed to influence the behaviour, attitudes and emotions of target foreign audiences.[28] Psychological operations "aim directly at the human brain" by drawing on historical, cultural, religious, ethical and other beliefs that affect people as individuals or groups.[29]

16. In September 1994, the United States waged an aggressive information campaign in Haiti aimed at convincing the military regime that its cause was futile and that it should step

---

[24] Pat Cooper, "Information Warfare Sparks Security Affairs Revolution," *Defense News*, 12-18 June 1998, p. 1.

[25] Tirpak, p. 34.

[26] Pat Cooper, "Information Warfare Changes the Way War is Waged," *Defense News*, 4-10 December 1995, p. 42.

[27] Cooper, "Pentagon Debates," 13-19 May 1996, p. 3.

[28] Gode Davis, "Space Jams and Quiet Knights: Special Military Operations," *Journal of Electronic Defense*, March 1998, p. 43.

[29] Gregory R. Copley, "Re-defining Psychological Strategy in the Age of Information Warfare," *Defense and Foreign Affairs Strategic Policy*, June 1998, p. 383.

aside peaceably in favour of the legitimate government.[30] More recently, in September 1997 an American psyops unit successfully threatened to jam electronically all radio and television broadcasts of ethnic Serb hardliners if they did not cease what the American unit characterized as "a persistent pattern of venomous rhetoric."[31] Controlling of television images in a closed society in order to provide its members with either misinformation or accurate information—depending on the circumstances—is also a form of psyops in that it could be used to discredit an enemy leader in the eyes of his people.

**Offensive and defensive information warfare**

17. *Joint Vision 2010* (1996), which provides the overall conceptual template for the future of America's armed forces, notes that achieving information superiority requires the waging of both offensive and defensive information warfare.[32] Much of what has been described above is *offensive information warfare*, that is, measures designed to exploit or degrade an adversary's ability to collect or use information. Offensive information warfare includes traditional methods, such as precision attacks to destroy an adversary's command and control capability, and nontraditional methods, such as attacking with computer viruses, infiltrating enemy information systems and managing information through media deception.

18. *Defensive information warfare* protects one's own ability to carry out information-based operations. Traditional defensive information warfare activities include physical security measures and encryption. Nontraditional actions will range from antivirus protection to innovative methods of secure data transmission.[33]

19. The May 1997 Quadrennial Defense Review notes that, to date, the US Department of

---

[30] David L. Grange and James A. Kelley, "Victory Through Information Dominance," *Army*, March 1997, p. 34.

[31] Davis, p. 43.

[32] *Joint Vision 2010*, p. 16.

[33] Ibid.

Defense has directed most of its information warfare efforts to protecting the military's growing network of information systems from attack. But the Review goes on to state that offensive actions designed to disrupt an adversary's access to information are also part of US military capabilities, and that such capabilities will be increased in future to ensure US information superiority during a conflict. For its part, Canada remains primarily focused on defensive information warfare.[34]

## US SERVICE VISIONS AND INFORMATION WARFARE

20. The US armed services have incorporated aspects of information warfare into all of their recent defence statements and visions. *Joint Vision 2010* sees information superiority as the foundation upon which four key battle winning concepts—dominant manoeuvre, precision engagement, focused logistics and full-dimensional protection—will be built. *Global Engagement: A Vision for the 21st Century Air Force* (1996) identifies information superiority as the fifth of its six core competencies, which also include air and space superiority, global attack, rapid global mobility, precision engagement and agile combat support. In 1997 the Air Force opened an information warfare battlelab designed to improve capabilities related to this core competency.

21. *Army Vision 2010* (1996) focuses on the land aspects of dominant manoeuvre, precision engagement, full-dimensional protection, focused logistics and information superiority. Information superiority is central to the Army's quest to create a "digitalized" battlefield by 2020. Under this plan, which is part of its Force XXI initiative, the US Army aims to equip each soldier and vehicle with a small computer that will display a map of the battlefield overlaid with friendly and enemy positions and aircraft flight paths. Finally, in *Forward from the Sea* (1994), the US Navy identifies five fundamental roles: sea control and maritime supremacy, power projection from sea to land, strategic deterrence, strategic lift and forward naval presence.

---

[34] Sharon Hobson, "Canada's Information Ops in Defensive Role," *Jane's Defence Weekly*, 15 October 1997, p. 29.

Although these roles are not new, the way in which they are to be carried out will be. The Navy has embraced the concept of "network-centric warfare" to achieve information superiority. This concept places greater emphasis on the sensor and surveillance systems of a group of warships, submarines or aircraft, rather than on the particular attributes of the platform itself.[35]

## IS INFORMATION WARFARE NEW?

22. Many observers point out that much of what has been described so far as information warfare is not new. Military commanders have always sought to achieve an information advantage over their adversaries, whether this came from knowledge of terrain or satellite imagery. Similarly, command and control warfare, electronic warfare and psychological warfare are long-established activities.

23. That said, information is now far more important to the outcome of a battle than it has been in the past. Whereas at one time intelligence collection was manpower- and time-intensive, today's sensing and reporting technologies offer an unprecedented degree of knowledge, often in real time. The overall effect is to shift the contribution of information from "preparing a battlefield to mastering a battlefield".[36] Thus, although armies have conducted "information warfare" operations throughout history, today's expanded methods and capabilities make information distinctly more important, effective and necessary for successful operations.

24. Some experts argue that information warfare is becoming an alternative to more traditional forms of war. This notion holds that information itself can be used as a weapon. By manipulating information through the use of computers, the Internet, satellite communications and television images, the case is made, one can directly influence the decisions of an enemy.[37]

---

[35] Robert Holzer, "US Navy Steps Up Data-Linked Warfare Pace," *Defense News*, 10–16 November 1997, p. 8.

[36] Libicki.

[37] R. L. DiNardo and Daniel J. Hughes, "Some Cautionary Thoughts on Information Warfare," *Airpower Journal*, Winter 1995, p. 70.

25. Others dispute this view. They note that while the collection of information can be impeded and its movement frustrated, it is becoming easier to acquire, store, and communicate information.[38] Using networked microcomputers, an enemy leader can disperse his command centres to many locations, making it very difficult for an attacker to destroy them all.[39] Thus, although a computer network attack could play a supporting role in certain conflicts, it likely would not be decisive in itself.[40] Moreover, with its unknown effects and unknown collateral damage, information warfare is an imprecise weapon that would not seem attractive in an arsenal which, in all other respects, is becoming ever more precise.[41] For Martin Libicki, an information warfare specialist at the National Defence University, the notion of information warfare as a separate element of war is "grossly exaggerated."[42]

26. From this perspective, information warfare represents an extension of the traditional importance of obtaining and using information in war. It is not intended to replace conventional troops, fighter planes or ships, but rather, to assist and supplement traditional military offence and defence.[43] Information warfare, in this view, will not replace traditional warfare but simply enhance the way in which war is waged.[44]

## INFORMATION OPERATIONS

27. In recent years, the Canadian Forces has come to realize that the pervasiveness of information technology is such that its role needs to be understood not just in terms of actual warfighting but also in the context of the broader information environment. The Canadian Forces Information Operations doctrine document defines information operations as actions taken in support of political and military objectives which influence decision makers by

---

[38] Lawrence Freedman, "Computers, Viruses and War," *Newsweek*, 27 April 1998, p. 4.

[39] "Cyberwar Threat Real and Growing," *Aviation Week and Space Technology*, 27 April 1998, p. 78.

[40] Freedman, p. 4.

[41] *Economist* Survey on Defence Technology, p. 19.

[42] Libicki.

[43] Peter Hum, "Preparing for Cyberwar," *Ottawa Citizen*, 20 March 1997.

[44] Pat Cooper, "C3I, Data Become Battlefield Targets," *Defense News*, 4-10 December 1995, p. 8.

affecting others' information while exploiting and protecting one's own information.[45] Such actions might include a computer network attack on civilian systems (discussed below), a public affairs campaign or, if the confrontation has escalated to a conflict, the information warfare techniques discussed above. A good example of a successful public affairs campaign is Brian Tobin's "turbot war" in the summer of 1995. Somali warlord Mohammed Farrah Aidid also waged a "successful" information operations campaign when his forces dragged an American soldier through the streets of Mogadishu.

28. The Canadian Forces doctrine document goes on to note that the strategic aim of information operations is to secure peacetime national security objectives, deter conflict, protect Canadian Forces information and information systems and shape the information environment. If deterrence fails, Canada uses information operations to achieve information superiority and thereby attain its objectives against potential adversaries in times of crisis and/or conflict.[46] This is information warfare. Thus, information operations can be viewed as an overarching concept which subsumes information warfare as one of its components.[47]

**Computer network attack on civilian systems**

29. One aspect of information operations is the notion of a computer network attack on civilian computer-based systems. Many military and intelligence officials in the United States and Canada believe that a computer network attack on civilian systems is a distinct possibility. Potential targets include electrical power grids, telephone systems, stock markets, financial centres and the air traffic control system. Possible attackers range from hostile national intelligence and military organizations to terrorists, criminals, industrial competitors and disgruntled or disloyal insiders.[48]

---

[45] *Canadian Forces Information Operations*, B-GG-005-004/AF-032, 4 April 1998, p. 1-2/14.
[46] Ibid., p. 1-1/14.
[47] *Global Challenges and Opportunities*, Canada 2005 Doc., Summer 1998, p. 23.
[48] Tirpak, p. 33.

30. The prospect of a computer network attack on civilian systems serves to blur the distinction between the military and civilian spheres. Just as air raids on London during World War II forced civilians to become part of the battle, so too with information operations the civilian sector is no longer a sanctuary that can be protected by interposing military forces between threats or adversaries and their targets.[49] Even more so with information operations, however, geographical distance is truly rendered irrelevant, as targets within one's home country become just as vulnerable as targets in theatre.[50] In this sense, information operations have no front line: potential battlefields exist wherever networked systems allow access.[51]

31. A computer network attack on civilian systems could have direct military implications. American defence experts have noted that nearly everything the US military does—from designing weapons systems and guiding missiles to paying, training, equipping and mobilizing soldiers—depends on computer-driven civilian information networks.[52] Over 95 per cent of US military communications during peacetime travel over the same phone lines used by civilians.[53] American military bases are powered by the national electric power grid. Pentagon purchases are conducted via the federal banking network. Soldiers are transported on aircraft directed by civilian air traffic control towers. In short, "if the civilian computers stopped working, America's armed forces couldn't eat, talk, move or shoot."[54] The Canadian Forces faces a similar set of dependencies and challenges—although Canada's military network is inherently more secure since, unlike its US counterpart, the Canadian Forces does not rely on the Internet for communications.

---

[49] Richard E. Hayes and Gary Wheatly, "Information Warfare and Deterrence," *Institute for National Strategic Studies Strategic Forum*, October 1996, http://www.ndu.edu/ndu/inss/strforum/forum87.html.

[50] Roger C. Molander, Andrew S. Riddile and Peter A. Wilson, "Strategic Information Warfare: A New Face of War," *Parameters*, Autumn 1996, http://carlisle-www.army.mil/usawc/Parameters/96autumn/molander.htm.

[51] "Information Warfare and Cyberspace Security," *Rand Research Review*, Fall 1995, http://www.rand.org/publications/RRR/RRR.fall95.cyber/infor_war.html.

[52] Ibid.

[53] *Information Operations*, p. 1-8.

[54] Munro, 16 July 1995, p. C3.

**Threats and vulnerabilities**

32. Most defence analysts accept that advanced military forces and societies are depending as never before on information systems, and that with this dependence comes vulnerabilities that an opponent could exploit. Some defence analysts go so far as to argue that information warfare could be "the great equalizer" between richer and poorer countries, since potential enemies, unable to match the sophisticated technologies of the United States and other Western nations, could respond "asymmetrically" using the relatively cheap technologies of information warfare. "You don't have to be big and rich to apply the kind of judo you need in information warfare," argues futurist Alvin Toffler.[55] But just how vulnerable are military and civilian systems to an information warfare attack?

33. *Threats to military information systems.* US war games have indicated that by 2025, or perhaps earlier, the US space systems upon which much of America's intelligence-based warfare is dependent could be at risk.[56] Threats include the physical disruption and destruction of satellites using small ground-based lasers or kinetic-energy systems, as well as electronic jamming and network attack by computer hackers. Others have argued that US satellite vulnerability has been exaggerated, and that it would be quite difficult to knock out communications and intelligence-gathering satellites.[57] Nonetheless, military planners are taking the threat seriously enough to consider a number of possible protective measures, including installing protective weapons and surveillance systems on satellites, shielding internal electronics to protect against attack, and improving satellite capabilities to function in an electronic jamming situation.[58]

34. Electronic jamming poses perhaps a greater threat to military systems than physical

---

[55] As quoted in Douglas Waller, "Onward Cyber Soldiers," *Time*, 21 August 1995, p. 35.

[56] Barbara Starr, "War Games Highlight US Vulnerability in Space," *Jane's Defence Weekly*, 8 October 1997, p. 17.

[57] George L. Seffers, "Army Urges Satellite Treaty," *Defense News*, 16-22 June 1997, p. 83

[58] Ibid.

destruction. Today military wireless communications attempt to overcome electronic warfare by spreading the message across a wide band of the spectrum, and hopping from frequency to frequency. This, however, does not make them invulnerable to technologies that are designed to locate transmissions and jam messages through a variety of means.[59]

35. As for a computer network attack, most defence analysts agree that it is more difficult to attack military combat systems than civilian targets. Their communication lines are more secure, and they usually have unique programming unfamiliar to most hackers. Viruses are not much use, experts say, because they probably will not work due to the unfamiliar system.[60] Nonetheless, the US services are not taking any chances. Because computer-based systems are central to the US Army's efforts to create a "digitalized army", it has established a Computer Emergency Response Team to solve the service's computer security problems around the world. The Army is also developing a Tactical Internet which, unlike its civilian counterpart, uses a combination of satellites and radios rather than phone lines to transmit information.[61] The US Navy has established a response team similar to the Army's, while the Air Force has created an entire Information Warfare Squadron. Formed to provide a deployable counter-information warfare capability, the Squadron will move with Air Force units, protecting the information systems set up at expeditionary sites and advising the theatre commander of the threats facing him in the information warfare context.[62] The Quadrennial Defense Review calls for a "robust commitment"—and increased funding—to protecting military information systems and computer networks from attack.

36. *Threats to civilian information systems*. Because they are designed for public access, civilian systems are comparatively easier to penetrate than military ones. "A few very smart

---

[59] *Economist* Survey on Defence Technology, p. 11.

[60] Michael A. Dornheim, "Bombs Still Beat Bytes," *Aviation Week and Space Technology*, 19 January 1998, p. 60.

[61] George Seffers, "US Army Forms Crisis Team to Fight Hackers," *Defense News*, 24-30 March 1997, p. 23.

[62] Tirpak, p. 34.

guys with computer workstations and modems could endanger lives and cause great economic disruption," argues a former Pentagon communications specialist.[63] Other experts believe that the threat of civilian computer network attack may be overstated. An April 1997 US Defense Science Board report concluded that the conduct of strategically important information warfare "is not a trivial exercise of hacking into a few computers", as is the common perception. Although it is relatively easy for skilled individuals to break into unprotected and poorly configured networked computers, it is much more difficult to mount an attack on complex systems that would cause crucial damage.[64]

37. Besides the difficulty of figuring out how to corrupt a complex system, the prospect of a massive disruption is lessened by the growing redundancies incorporated into civilian information systems. As is the case with their military counterparts, civilian systems are becoming more dispersed and redundant, and therefore less susceptible to widespread damage.

38. Technology's "immune systems" are also being improved to counter a network attack. Modern computers are being built with safeguards to prevent tampering, and data encryption methods are being developed that are seemingly indecipherable.[65] For Libicki, digital technologies will make "spoofing"—substituting deceptive messages for valid ones—nearly impossible.[66]

39. *Private sector perspective.* Although civilian systems are at greater risk than their military counterparts, and the means for making them more secure are available, relatively little has been done to guard them against network attack. This is in part because business leaders and some policy makers are ambivalent about the wisdom of broadcasting their vulnerability. Industry executives are hesitant to cooperate with other firms and with the government on

---

[63] Donald Latham as quoted in Waller, p. 35.

[64] "Sharing the Knowledge," *International Defense Review*, 1 April 1997, p. 4.

[65] Bruce Ward, "Mac Attack: American Strategists Girding for War but Cyberspace is the New-Age Arena," *Ottawa Citizen*, 19 April 1998, p. D11.

[66] Libicki.

computer security matters for fear that the disclosure of an intrusion would undermine public confidence in their business. Similarly, government officials rarely discuss penetrations of government networks. This reluctance to discuss computer intrusions has undercut the development of a common defence against the feared future attack on civilian systems.[67]

40. A second point is that some private sector executives are not entirely convinced of the urgency of the threat. They note that while reports abound of computer hackers successfully penetrating secure government and business networks, they know of no computer network attack that has caused a serious breach of national security. With no catastrophic incident to indicate a cause for alarm, the civilian world—which owns and operates most of the networks that would be prime targets in a computer network attack—has not taken the threat as seriously as have military and intelligence officials.

41. *Military and intelligence perspective.* Military and intelligence officials disagree with the private sector's assessment of the threat. For CIA Director George Tenet, the threat of civilian systems being disrupted "is real and growing".[68] Indeed, the evidence shows that government and private industry systems in the United States and Canada are constantly under systematic and organized attack.[69] In July 1998 the CIA Director said before Congress that at least a dozen countries, some hostile to America, are developing programs to attack other nations' information and computer systems.[70] A recent US study predicts that by 2005 organized criminals, terrorists and foreign spies will be launching widespread attacks on vital US information infrastructures.[71] If so, Canada would clearly be vulnerable because its infrastructure is closely linked to US networks.

---

[67] Bradley Graham, "Lack of Disclosure Impedes Development of Safeguards," *Washington Post*, 28 February 1998, p. A6.

[68] "Cyberwar Threat Real and Growing," *Aviation Week and Space Technology*, 27 April 1998, p. 78.

[69] Canadian Defence Science Advisory Board Report Information Operations (97/1).

[70] Douglas Pasternak, "Terrorism at the Touch of a Keyboard," *US News & World Report*, 13 July 1998, p. 37.

[71] Peter Hum, "Defending Canadian Cyberspace: DND Seeks to Co-ordinate Battle Plan with Spy Agency and Mounties," *Ottawa Citizen*, 22 March 1997.

**Deterring computer network attack**

42. One possible response to the prospect of a computer network attack on civilian systems is to take measures to deter such action. Deterrence relies on placing one's opponent at a great enough risk to dissuade him from contemplating an attack. The most obvious means of deterrence in this case is to threaten one's opponent with the prospect of a retaliatory computer network attack. This approach, however, assumes that the opposing state places as great a value on civilian information systems as does one's own—and at present the Western world is much more dependent on such systems than are other societies. From this perspective, there is some truth to the *Economist*'s tongue-in-cheek observation that the West's "best defence is to encourage potential enemies to become equally dependent on information technology. Then there would be scope for retaliation."[72]

43. A second problem is that a retaliatory computer network attack may have adverse effects on the deterrer. The nature of high-tech networks is such that they are not a nationally bounded asset. Information technology has created such a high degree of connectivity among nations that it is often difficult, if not impossible, to separate out disruptions between national and global levels.[73] Depending on the target, therefore, responding with a computer network attack may be the equivalent of shooting oneself in the foot. As a result, any means of retaliation is likely to depend to large degree on traditional military instruments.[74]

44. The third and most significant problem with a deterrence strategy based on "retaliation in kind" is that the attack may not emanate from a state at all. The technology is such that small groups—terrorists, organized criminals and hackers—may now have the capability to wreak a degree of damage that once belonged only to states.[75] Such groups and individuals are unlikely

---

[72] "Cyber wars," *Economist*, 13 January 1996, p. 77.

[73] Richard J. Harknett, "Information Warfare and Deterrence," *Parameters*, Autumn 1996, http://carlisle-www.army.mil/usawc/Parameters/96autumn/harknett.htm.

[74] Molander, Riddile and Wilson.

[75] Harknett.

to be deterred by the prospect of a retaliatory computer network attack since it is highly unlikely improbable that they are dependent on civilian information systems as a state. Moreover, deterrence requires that the opponent be identifiable, and this may not be possible in the case of a computer network attack.

**Defending against computer network attack**

45. Because deterring a computer network attack is so problematic, most governments have focused on the denial aspect of deterrence. Both the United States and Canada have undertaken initiatives to increase the security of civilian infrastructures. In 1996 US President Clinton created a Commission on Critical Infrastructure Protection to examine possible physical and electronic threats to critical infrastructures such as energy, banking and finance, transportation, vital human services and communications. In April 1998 the President issued a directive implementing the Commission's key recommendations, including the creation of an Office of National Infrastructure Assurance within the National Security Council.[76] In devising the government's policy to counter against civilian computer network attack, Clinton decided against prescribing computer protection measures for the private sector. Instead, he is counting on self-interest to spur companies to identify their vulnerabilities and install improved detection systems.[77] Meanwhile, the Pentagon has established an Information Operations Working Group to address defence-related issues of infrastructure protection.

46. Canada, too, has begun to think seriously about information operations. The Department of National Defence and the Canadian Forces have undertaken a number of initiatives in this area. DND has approved a doctrine document on Canadian Forces Information Operations providing guidance on all aspects of information operations. A Canadian Forces Information Operations Group has also been created and in the summer of 1998 it established both a

---

[76] George Seffers, "Clinton Prepares Infowar Response," *Defense News*, 16-22 March 1998, p. 1.

[77] "Clinton on Infrastructure: Too Little Too Late?" *Computergram International*, 26 May 1998, p. CGN05260034.

Network Vulnerability Assessment Team and a Computer Instant Response Team. In addition, Canada is participating in the Pentagon's working group on information operations, and the Canada-US Military Cooperation Committee has set up a similar working group.[78]

47. As the distinction between the military and civilian spheres becomes blurred in the information age, so too do the jurisdictions and responsibilities of various governmental agencies. A computer network attack on civilian infrastructure could have direct military implications, thereby obscuring the distinction between the traditional roles of domestic law enforcement and national security. In Canada, this could lead to confusion over the division of responsibilities among the RCMP, the Communications Security Establishment, the Canadian Security and Intelligence Service, the Canadian Forces and the Department of National Defence. For its part, the Department of National Defence has stressed that when it comes to infrastructure protection, its responsibilities are limited to defence works, establishments, facilities, assets, resources and operations, in Canada and abroad. The Department has consistently advocated a strong centrally based leadership role for the Privy Council Office in the area of infrastructure protection.[79]

## CONCLUSION

48. Information technology is increasingly central to both the efficient prosecution of military operations and the smooth functioning of civilian life. As advanced societies become ever more dependent on information, vulnerabilities arise which an opponent could exploit. Although in some cases these vulnerabilities will lie directly within the military or civilian spheres, the nature and pervasiveness of information technology is such that the boundaries between domestic law enforcement and national security will often become blurred. The challenge of the future is not only to find effective responses to, and ways of conducting,

---

[78] Howard C. Dickson, DND Chief Information Officer, memo critiquing the Defence Science Advisory Board Report on Information Operations (97/1), 16 July 1998.

[79] Dickson memo, 16 July 1998.

information operations, but also to define the responsibilities and identify the appropriate agencies for carrying out these tasks.

DOCUMENT CONTROL DATA
(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

1 ORIGINATOR (the name and address of the organization preparing the document Organizations for whom the document was prepared e.g Establishment Sponsoring a contractor's report, or tasking agency, are entered in Section 8)

Directorate of Strategic Analysis
14 NT MGen Pearkes Bldg
Ottawa, Ont. K1A 0K2

2 SECURITY CLASSIFICATION
(overall security classification of the document, including special warning terms if applicable)

UNCLASSIFIED

3 TITLE (the complete document title as indicated on the title page Its classification should be indicated by the appropriate abbreviation (S, C or U) in parentheses after the title)

Information Warfare and Information Operations

4 AUTHORS (last name, first name, middle initial)

Sloan, Elinor C

5 DATE OF PUBLICATION (month Year of Publication of document)

October 1998

6a NO OF PAGES (total containing information. Include Annexes, Appendices, etc.)
20

6b NO OF REFS (total cited in document)

79

7 DESCRIPTIVE NOTES (the category of document, e g technical report, technical note or memorandum. If appropriate, enter the type of report e.g interim, progress, summary, annual or final Give the inclusive dates when a specific reporting period is covered.)

D Strat A Research Note 98/09

8 SPONSORING ACTIVITY (the name of the department project office or laboratory sponsoring the research and development. Include the address)

Directorate of Strategic Analysis

9a. PROJECT OR GRANT NO. (if appropriate, the applicable research and development project or grant number under which the document was written Please specify whether project or grant.)

N/A

9b CONTRACT NO. (if appropriate, the applicable number under which the document was written.)

N/A

10a ORIGINATOR's document number (the official document number by which the document is identified by the originating activity. This number must be unique to this document )

N/A

10b. OTHER DOCUMENT NOS (Any other numbers which may be assigned this document either by the originator or by the sponsor )

N/A

11 DOCUMENT AVAILABILITY (any limitations on further dissemination of the document, other than those imposed by security classification.)
(x ) Unlimited distribution
( ) Distribution limited to defence departments and defence contractors· further distribution only as approved
( ) Distribution limited to defence departments and Canadian defence contractors; further distribution only as approved
( ) Distribution limited to government departments and agencies; further distribution only as approved
( ) Distribution limited to defence departments; further distribution only as approved
( ) Other (please specify):

12. DOCUMENT ANNOUNCEMENT (any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11) However, where further distribution (beyond the audience specified in 11) is possible, a wider announcement audience may be selected.)

None

13. ABSTRACT (a brief and factual summary of the document It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual)

This report begins by looking at the definition, objective and forms of information warfare. It then discusses the role of information warfare in military operations before turning to the broader concept of information operations Here the paper focuses on the prospect of a computer network attack on civilian infrastructures and how governments are responding The report concludes that the challenge of the future is not only to find effective responses to, and ways of conducting, information operations, but also to define the responsibilities and identify the appropriate agencies for carrying out these tasks.

En premier lieu, ce rapport présente la définition, l'objectif et les diverses formes de la guerre de l'information Il explique ensuite le rôle que joue la guerre de l'information dans les opérations militaires, puis décrit le concept plus large des opérations d'information. Il se poursuit en abordant l'éventualité d'une attaque des réseaux informatiques appartenant aux infrastructures civiles et la façon dont les gouvernements s'y préparent Le rapport conclut que la lourde tâche qu'il faudra accomplir au cours des prochaines années consistera non seulement à trouver des moyens d'agir efficacement face aux opérations d'information et de mener ce genre d'opérations, mais aussi à définir les responsabilités en la matière et à déterminer les organismes qui pourront relever ce défi.

14 KEYWORDS, DESCRIPTORS or IDENTIFIERS (technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document They should be selected so that no security classification is required Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included If possible keywords should be selected from a published thesaurus, e g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus-identified If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title )

Information Warfare
Information Operations
Revolution in Military Affairs
Strategic Studies